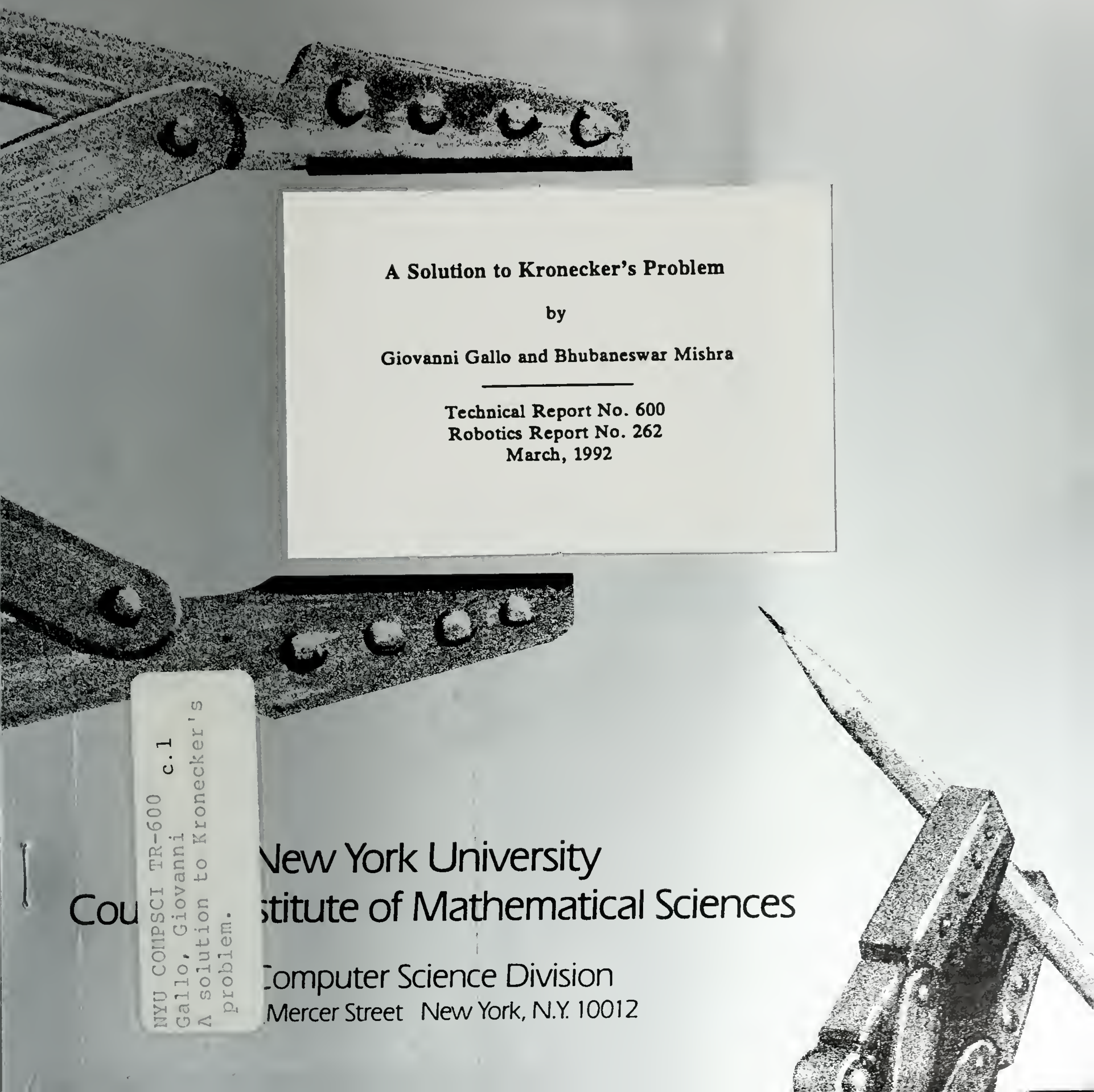
Robotics Research Technical Report



A Solution to Kronecker's Problem

by

Giovanni Gallo and Bhubaneswar Mishra

Technical Report No. 600
Robotics Report No. 262
March, 1992

NYU COMPSCI TR-600 c.1
Gallo, Giovanni
A solution to Kronecker's
problem.

New York University
Cou stitute of Mathematical Sciences

Computer Science Division
Mercer Street New York, N.Y. 10012

A Solution to Kronecker's Problem

by

Giovanni Gallo and Bhubaneswar Mishra

Technical Report No. 600
Robotics Report No. 262
March, 1992

New York University
Dept. of Computer Science
Courant Institute of Mathematical Sciences
251 Mercer Street
New York, New York 10012

Work on this paper has been supported by NSF grant #CCR-90-02819, ONR grant #N00014-89-J3042 and NYU Dean's Dissertation Fellowship

A Solution to Kronecker's Problem

Giovanni Gallo
Bhubaneswar Mishra

Courant Institute, New York University

1. Introduction

"Kronecker believed God made the natural numbers and all the rest was man's work. We only know of this opinion by hearsay evidence[1], however, and his paper *Über den Zahlbegriff* indicates to me that he thought God made a bit more: *Buchstabenrechnung*, or calculation with letters[2]. In modern terms, Kronecker seems to envisage a cosmic computer which computes not just with natural numbers, but with polynomials with natural number coefficients (in any number of indeterminates). That's the God-given hardware. The man-made software then creates negative numbers, fractions, algebraic irrationals, and goes on from there. Kronecker believed that such a computer, in the hand of an able enough programmer, was adequate for all the purposes of higher mathematics[3]."

The preceding notion of constructive mathematics, as postulated by Kronecker, can be expanded further and leads to some very interesting algorithmic problems. While it is quite apparent that Kronecker regarded these algorithmic questions as at the heart of his formulation of mathematics[4], it is unclear whether Kronecker had been able to resolve these questions in a satisfactory manner. Edwards, in his essay on Kronecker's views[5], has the following to say: "I find no such algorithm in his works. My best guesses as to the explanation of this paradox is that he had an algorithm which he had not yet reduced to a form ready to publish, or, perhaps, that he had an algorithm in many cases but had not yet found one in the general case. Or, as is entirely possible, it lies somewhere in his voluminous collected works waiting to be found."

The present notes make a fresh attempt at resolving the algorithmic questions raised by Kronecker, while remaining faithful to the notion of constructivity espoused by Kronecker. Furthermore, we attempt to stay close to the approaches and concepts that were known and available to Kronecker. In order to avoid confusion, however, we shall use modern algebraic terminology.

To understand Kronecker's notion of constructivity, we need a detailed look at the latent algorithmic questions: According to Kronecker, the semi-ring $\mathbb{N}[x_1, x_2, \ldots, x_n]$[6] is God-given—-at least, a finite but significantly large fraction of it is God-given. The man-made algorithms can then carry out all computations using the elements of $\mathbb{N}[x_1, x_2, \ldots, x_n]$, i.e., using only the natural numbers and letters. Thus, even though we think of infinite sets, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, and computations involving the elements of these sets, we must treat all calculations as occurring

[0] Supported by NSF Grant #CCR-90-02819 and ONR Grant #N00014-89-J3042, and NYU Dean's Dissertation Fellowship.

Authors' Address: Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY-10012.

[1] H. Weber. *Leopold Kronecker*, Jahresber. D.M.-V., **2**:19, (1892).

[2] *Leopld Kronecker's Werke*, (von K. Hensel), **3**: Leipzig, Druck und Verlag von B.G. Teubner, (1895).

[3] Harold M. Edwards. *Kronecker's Views on the Foundations of Mathematics*, "Proceedings of a Conference held at Vassar College in June 1988," (D. Rowe and J. McCleary, eds.), Academic Press, (1990).

[4] *Werke*.

[5] *Kronecker's Views on the Foundations of Mathematics*.

[6] Here, $\mathbb{N}$ denotes the set of *natural numbers*: $\{0, 1, 2, \ldots\}$ and $\mathbb{N}[x_1, x_2, \ldots, x_n]$ denotes the set of multivariate polynomials with coefficients from $\mathbb{N}$ and in variables $x_1, x_2, \ldots, x_n$. Both $\mathbb{N}$ and $\mathbb{N}[x_1, x_2, \ldots, x_n]$ are *semi-rings*—rings except that subtraction may not always be possible.

with a finite subset of $\mathbb{N}$ and finitely many letters x_1, x_2, ..., x_n—as if, the computations over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc. get *compiled* into the *low-level* programs involving $\mathbb{N}[x_1, x_2, \ldots, x_n]$ and then *executed*.

A concept basic to the Kronecker's *programme* is the idea of equivalence of two elements, A and A' of $\mathbb{N}[x_1, x_2, \ldots, x_n]$ *modulo* a finite collection $\{M_1, M_2, \ldots, M_\nu\} \subset \mathbb{N}[x_1, x_2, \ldots, x_n]$. Namely,

Definition 1.1 Given A, A', $M_1, M_2, \ldots, M_\nu \in \mathbb{N}[x_1, x_2, \ldots, x_n]$, we say that $A \sim A' \bmod (M_1, M_2, \ldots, M_\nu)$ if for some $\phi_1, \phi_2, \ldots, \phi_\nu, \psi_1, \psi_2, \ldots, \psi_\nu \in \mathbb{N}[x_1, x_2, \ldots, x_n]$,

$$A + \sum_{i=1}^{\nu} \phi_i M_i = A' + \sum_{i=1}^{\nu} \psi_i M_i. \quad \square$$

If we apply the above definition to the special case of $\mathbb{N}[x]$ and $M_1 = 1 + x$ we see that any polynomial in $\mathbb{N}[x]$ is equivalent to one of the form $a + bx$ ($a, b \in \mathbb{N}$), since

$$\begin{aligned} x^2 + 1(1+x) &= 1 + x(1+x) \quad \text{and} \\ x^2 &\sim 1 \bmod (1+x). \end{aligned}$$

Furthermore, it is easily seen that the following are equivalent:

$$\begin{aligned} a + bx &\sim c + dx \bmod (1+x) \\ a + d + b(1+x) &\sim c + b + d(1+x) \bmod (1+x) \\ a + d &\sim c + b \bmod (1+x) \\ a + d &= c + b. \end{aligned}$$

Thus, the semi-ring of equivalence classes $\mathbb{N}[x]/(1+x)$ is *isomorphic* to the ring of integers $\mathbb{Z}$. Thus, after a preprocessing which amounts to equivalence modulo $1+x$ we can feel free to use any finite collection of integers as well as the natural numbers. Thus as we perform computations in $\mathbb{Z}$, we only need to remember that "$-b$" is really "bx" and after each operation, we do a straightforward normalization to bring the representation into the form "$a + bx$." Thus each ring operation over $\mathbb{Z}$ corresponds to some constant number of (perhaps, five) operations in $\mathbb{N}$. *For all practical purposes, God could have got us started with* $\mathbb{Z}$!!

In a similar way, by considering $\mathbb{N}[x, y_1, \ldots, y_n]/(1 + x, a_1 + b_1xy_1, \ldots, a_n + b_nxy_n)$, we can create any finite collection of rational numbers[7] as well. In general then, by using an arbitrary set of modulii we can perform arithmetic in any algebraic number field or even algebraic function field. In particular, the field of rational functions on an algebraic curve can be handled in this way.

[7] Quoting Edwards: "Our impulse is to go on to construct the field of rational numbers, but Kronecker does not, and, in fact, one cannot. One can throw in another indeterminate t [in addition to e] and another relation $1 + 10et$ (that is, two indeterminates e, t and two relations $1 + e$ and $1 + 10et$) to get the ring of all terminating decimal fractions. Similarly, one can construct rings of rational numbers containing any finite set of denominators, so any computation with rational numbers can be carried out, but the field of rational numbers as a complete infinite set cannot be described in the way we are used to doing it. But that would not have bothered Kronecker, for whom even the *natural* numbers were not a completed infinite set." (From *Kronecker's Views on the Foundations of Mathematics*)

Thus Kronecker's approach to the foundations of mathematics relies greatly on the problem of computing in semi-ring, that is, the problem of deciding whether two given A's are equivalent modulo a given set of M's. Edwards puts it as follows[8]:"Based on my reading of Kronecker over the years, I regard it as a certainty that he would have regarded it as essential that this problem—which he puts[9] at the heart of his formulation of mathematics—can be solved algorithmically, that is, by a computational procedure which can be shown to terminate after a number of steps for which an *a priori* (finite) upper bound can be given." Following our earlier discussions, we can then formulate *Kronecker's problem* as:

Problem 1.1 (Kronecker's Problem)

GIVEN: $A,\ A',\ M_1,\ M_2,\ \ldots,\ M_\nu \in \mathbf{Z}[x_1,\ x_2,\ \ldots,\ x_n]$.

DECIDE: *Whether* $A \sim A' \bmod (M_1,\ M_2,\ \ldots,\ M_\nu)$.

Additionally, we require a finite upper bound N (perhaps depending on the parameters n, ν, and $|A|$, $|A'|$, $|M_1|$, $|M_2|$, …, $|M_\nu|$[10]) on the the number of steps the decision procedure may require. □

Let us recast Kronecker's problem in the modern ideal theoretic language. Let $\mathcal{M}$ denote the ideal[11] generated by the set $\mathrm{M} = \{M_1,\ M_2,\ \ldots,\ M_\nu\}$, i.e.,

$$\begin{aligned}\mathcal{M} &= (M_1, M_2, \ldots, M_\nu)\\ &= \left\{\sum_{i=1}^{\nu} \theta_i M_i \mid \theta_i \in \mathbf{Z}[x_1, x_2, \ldots, x_n]\right\} \subset \mathbf{Z}[x_1, x_2, \ldots, x_n].\end{aligned}$$

Then Kronecker's problem is equivalent to the *ideal membership problem* for $\mathbf{Z}[x_1,\ x_2,\ \ldots,\ x_n]$, i.e., the problem of deciding if $A - A' \in \mathcal{M}$.

Problem 1.2 (Ideal Membership Problem)

GIVEN: *An ideal* $\mathcal{M} = (M_1,\ M_2,\ \ldots,\ M_\nu) \subset \mathbf{Z}[x_1,\ x_2,\ \ldots,\ x_n]$ *and a polynomial* $A \in \mathbf{Z}[x_1,\ x_2,\ \ldots,\ x_n]$.

DECIDE: *Whether* $A \in \mathcal{M}$.

As before, we require a finite upper bound N (perhaps again depending on the parameters n, ν, and $|A|$, $|M_1|$, $|M_2|$, …, $|M_\nu|$) on the the number of steps the decision procedure may require[12]. □

[8] *Kronecker's Views on the Foundations of Mathematics.*

[9] *Werke.*

[10] If $M = \sum_{\langle e_1,\ldots,e_n\rangle \in \mathbf{N}^n} a_{\langle e_1,\ldots,e_n\rangle} x_1^{e_1} \cdots x_n^{e_n} \in \mathbf{Z}[x_1, \ldots, x_n]$ then by $|M|$ we denote the upper bound on all the coefficients, $|a_{\langle e_1,\ldots,e_n\rangle}|$'s, and the all the degrees in each variable, e_i's and call it the *size* of the polynomial M. Thus, $|M|$ is simply the larger of the largest coefficient in M (in its absolute value) and its degrees in each variable.

[11] In Kronecker's language an ideal would be called a *modulsysteme*. In light of our earlier discussions, Kronecker's terminology is quite appropriate.

[12] Given $A,\ M_1,\ M_2,\ \ldots,\ M_\nu \in \mathbf{Z}[x_1,\ x_2,\ \ldots,\ x_n]$, let

$$\Theta = \{\langle \theta_1, \ldots, \theta_\nu \rangle : A = \theta_1 M_1 + \cdots \theta_\nu M_\nu\}.$$

The *ideal membership problem* has received considerable attention from the constructive/computational algebra community resulting in algorithms that proceed in the spirit of "Gröbner-Buchberger" basis formulation. The ideals of $\mathbf{Z}[x]$ had been studied much prior to the current work; Kronecker and Hensel enumerated[13] them in 1901. Starting in the early fifties, in a number of research papers, Szekeres[14] defined a canonical basis and used them to obtain invariants and to enumerate the ideals easily. Later, Szekeres[15] and Trotter[16] extended Szekeres' results to $\mathbf{Z}[x, y]$. The canonical bases, thus formed, have the following important property: *Each ideal $\mathcal{M}$ has a unique basis $T(\mathcal{M})$ so that the ideals $\mathcal{M}_1$ and $\mathcal{M}_2$ are equal if and only if* $T(\mathcal{M}_1) = T(\mathcal{M}_2)$. However, there was no algorithm that would compute such a canonical basis for an ideal $\mathcal{M} = (\mathrm{M})$ from a finite system of generators M of $\mathcal{M}$. Such an algorithm would actually solve our *ideal membership problem*, since $A \in \mathcal{M}$ if and only if $(\mathrm{M} \cup \{A\}) = (\mathrm{M})$. In 1978, Sims[17] introduced a simple algorithm from which a canonical basis of Szekres and Trotter could be obtained easily. Subsequently, Christine Ayoub[18] has generalized the ideas in Sim's algorithm to compute a canonical basis for an ideal in $\mathbf{Z}[x_1, x_2, \ldots, x_n]$.

In a related development, several researchers have investigated the *detachability* property of $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ (a notion first introduced by Richman[19]). A ring R is said to be *detachable*, if it allows an effective procedure to decide whether an element $f \in R$ belongs to an ideal $I \subseteq R$. That the ring $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ is detachable has been established by several authors (Simmons[20] in 1970, Richman[21] in 1974 and Seidenberg[22] in 1974). Actually, Simmons' procedure to determine if a polynomial $A \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$ is in the ideal $\mathcal{M}$ generated by $M_1, M_2, \ldots, M_\nu$, proceeds via two semi-decision procedures: the first terminates if $A \in \mathcal{M}$ and the second terminates if $A \notin \mathcal{M}$.

The third development in this direction comes from an attempt to generalize Buchberger's

Let

$$N' = \begin{cases} \min\{\max\{|\theta_1|, \ldots, |\theta_\nu| : \langle\theta_1, \ldots, \theta_\nu\rangle \in \Theta\}\}, & \text{if } \Theta \neq \emptyset; \\ -\infty, & \text{otherwise.} \end{cases}$$

Since an *a priori* knowledge of N' provides a decision procedure for the membership problem (using brute-force search) as well as an upper bound on the number of steps (for instance one can safely choose $N = (2\nu)^{(3N')^{(2N')^n}}$), a solution to the problem of estimating N' also provides a solution to the *ideal membership problem*. The problem in this form seems to have been first posed by D. Lazard in an electronic bulletin board message.

[13] L. Kronecker and K. Hensel. *Vorlesungen über Zahlentheorie*, Leipzig, (1901).

[14] G. Szekres. *A Canonical Basis for the Ideals of a Polynomial Domain*, *American Mathematical Monthly*, **59** (1952), pp. 379–386.

[15] G. Szekres. *Metabelian Groups with Two Generators*, in "Proceedings, International Conference Theory of Groups (Canberra, 1965)," Gordon and Breach, (1967), pp. 323–346.

[16] P.G. Trotter. *Ideals in $\mathbf{Z}[x, y]$*, *Acta Math. Acad. Sci. Hungar*, **32:12**, (1978), pp. 63–73.

[17] C. Sims. *The Role of Algorithms in the Teaching of Algebra*, in "Topics in Algebra," (M.F. Newman, Ed.), Springer-Verlag Lecture Notes in Mathematics, **697**, Canberra: Proc 1978, Springer-Verlag, New York, Berlin, (1978), pp. 95–107.

[18] Christine W. Ayoub. *On Constructing Bases for Ideals in Polynomial Rings over the Integers*, *Journal of Number Theory*, **17**, (1983), pp. 204–225.

[19] F. Richman. *Constructive Aspects of Noetherian Rings*, *Proc. American Mathematical Society*, **41:2**, (1974), pp. 436–441.

[20] H. Simmons. *The Solution of a Decision Problems for Several Classes of Rings*, *Pacific Journal of Mathematics*, **34** (1970), pp. 547–557.

[21] F. Richman. *Constructive Aspects of Noetherian Rings*, *Proc. American Mathematical Society*, **41:2**, (1974), pp. 436–441.

[22] A. Seidenberg. *What is Noetherian?*, *Rend. Sem. Mat. Fis. Milano*, **44** (1974), pp. 55–61.

algorithm for computing Gröbner basis of an ideal. The algorithm we present in these notes shares many ideas from Buchberger-Gröbner theory and could be classified to belong to this line development. In the original theory developed by Buchberger[23], he studied the bases for ideals in $K[x_1, x_2, \ldots, x_n]$, where K is a field. His original motivation was to study the quotient ring $K[x_1, x_2, \ldots, x_n]/J$, for some zero-dimensional ideal J. However, it has become quite apparent that the idea of a Gröbner basis of an ideal, an important concept in Bucheberger's theory, has many more applications than originally anticipated; in particular, one can provide an effective procedure to determine ideal membership in $K[x_1, x_2, \ldots, x_n]$ using a Gröbner basis. Several researchers (Zacharias[24] in 1978, Kandri-Rody and Kapur[25] in 1984, Lankford[26] in 1986) have generalized the concept of Gröbner basis for other commutative polynomial rings including $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ (as a special case of polynomial rings over an Euclidean domain). One of the authors[27] has investigated the characterization of the rings (termed, *strongly-computable rings*) over which such generalized Gröbner bases can be computed. Subsequently, we shall use many of the ideas used in these characterizations. As an immediate consequence of these generalizations, we also have effective procedures to determine if a polynomial $A \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$ is in the ideal $\mathcal{M}$ generated by $M_1, M_2, \ldots, M_\nu$.

However, while it is known that all these procedures for the *ideal membership problem* are effective (i.e., they eventually terminate), there has been no analysis of the time complexity for these algorithms. Thus, at the current state of knowledge, one is unable to provide an *a priori* bound on the number of steps any of these algorithms may take on a particular input. Still worse, the effectivity of these procedures can be shown using only non-constructive arguments, e.g., Dickson's Lemma, Hilbert's Basis Theorem or by *law of excluded middle* (Simmons' arguments depend on the assertion that either $A \in \mathcal{M}$ or $A \notin \mathcal{M}$). There have been many attempts to obtain a precise complexity of Buchberger's algorithm, but only in case of $K[x_1, x_2, \ldots, x_n]$ (where K is a field) the bounds are known. (In this case, there are fairly sharp upper and lower bounds[28].) A noteworthy attempt in this direction is due to Volker Weispfenning[29]. Using the

[23] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restclassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. Thesis, University of Innsbruck, Austria, (1965).

[24] G. Zacharias. *Generalized Gröbner Bases in Commutative Polynomial Rings*, B.Sc. Thesis, MIT, Cambridge (1978).

[25] A. Kandry-Rodi and D. Kapur. *Algorithms for Computing Gröbner Bases of Polynomial Ideals over Various Euclidean Rings*, *Lecture Notes in Computer Science*, **174** (1984), EUROSAM 84, International Symposium on Symbolic and Algebraic Computation, Cambridge, England, pp. 195–208.

[26] Dallas Lankford. *Generalized Gröbner Bases: Theory and Applications*, Technical Report, Louisiana Tech University, (1986).

[27] Bud Mishra. *Algorithmic Algebra*, To be published by Springer-Verlag, New York, (1992).

[28] D. Bayer and M. Stillman. *On the Complexity of Computing Syzygies*, *Journal of Symbolic Computation*, 6 (1988), pp. 135–147.

Thomas William Dubé. *Quantitative Analysis Problems in Computer Algebra: Gröbner Bases and the Nullstellensatz*, Ph.D. Thesis, Courant Institute of Mathematical Sciences, New York University, (1989).

D. Lazard. *Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations*, *Lecture Notes in Computer Science*, **162** (1983), Springer-Verlag, pp. 146–157.

E.W. Mayr and A.R. Meyer. *The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals*, *Advances in Mathematics*, **46** (1982), pp. 305–329.

C.K. Yap. *A New Lower Bound Construction for Commutative Thue Systems with Applications*, *Journal of Symbolic Computation*, **12** (1991), pp. 1–27.

[29] Volker Weispfenning. *Some Bounds for the Construction of Gröbner Bases*, Preprint, Mathematisches Institut

compactness theorem of first-order logic, he has shown the existence of recursive bounds for the Gröbner bases computation in the polynomial rings over a field, polynomial rings over a commutative regular ring and non-commutative polynomial rings of solvable type over a field. Unfortunately, his techniques do not apply to polynomial rings over $\mathbf{Z}$, and even if they did, the proof method would only provide a non-constructive argument as to the existence of such a bound.

Note added in proof: Recently, G. Moreno Socias has provided bounds similar to ours, *but for the ring of polynomials over a field.* The proof techniques are quite different from ours and are interesting on their own rights. Also, since the Moreno Socias' proofs are based on Macaulay's theorem, they can be considered constructive.

In these notes, we will first discuss an algorithm to solve the *ideal membership problem*, and then provide an upper bound on the number of steps it takes before terminating. The algorithm is quite similar to the Buchberger's algorithm for computing Gröbner bases. Additionally, we present some applications of our techniques to provide further bounds for a few related problems; in particular, our result yields an *effective Hilbert's Basis Theorem* for $\mathbf{Z}[x_1, x_2, \ldots, x_n]$.

2. Our Approach

In this section, we present an algorithm for the *ideal membership problem.* Our algorithm is similar to Buchberger's and Ayoub's algorithms in spirit. However, the main distinction is in the manner it deals with the reduction process. Each reduction step uses a "division" process very much like Buchberger's original algorithm for $K[x_1, x_2, \ldots, x_n]$ (K = a field) and shares some of the ideas proposed by Kronecker himself. In all other aspects, the algorithm is rather derivative in nature and is based on existing well-known concepts.

Let us assume a fixed but arbitrary order on the variables: $x_1 > x_2 > \cdots > x_n$. Let the ordering on the variables induce the lexicographic ordering on the *power products.* Thus

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \underset{\text{lex}}{>} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

if the first non-zero entry of the n-tuple

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) - (\beta_1, \beta_2, \ldots, \beta_n)$$

is positive. Note that the lexicographic ordering is a well-ordering[30].

Now consider an ideal $\mathcal{M} \subseteq \mathbf{Z}[x_1, x_2, \ldots, x_n]$ generated by a finite set $\mathrm{M} = \{M_1, M_2, \ldots, M_\nu\} \subset \mathbf{Z}[x_1, x_2, \ldots, x_n]$. Let $A \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$ be a multivariate polynomial with integer coefficients, whose terms are ordered according to the lexicographic ordering, with the biggest term occurring first. Following the usual terminology, we will denote the *leading power product* (or *head term*), *leading coefficient* (or *head coefficient*) and *leading monomial* (or *head monomial*) of A by Hterm(A), Hcoef(A) and Hmono(A), respectively. Thus,

$$\mathrm{Hmono}(A) = \mathrm{Hcoef}(A) \cdot \mathrm{Hterm}(A), \quad \text{where } \mathrm{Hcoef}(A) \in \mathbf{Z}.$$

der Universität, Heidelberg, Germany, (1987).

[30] It is possible to carry out the subsequent arguments *mutatis mutandis* with other *term* or *admissible orderings.* However, in order to keep our exposition simple, we have chosen to confine our discussions to the lexicographic ordering.

We also write, $A = \mathrm{Hmono}(A) + \mathrm{Tail}(A)$.

2.1 Head Reduction and E-Bases

Definition 2.2 (Head Reduction by M_i) If $\mathrm{Hmono}(M_i)$ divides $\mathrm{Hmono}(A)$ and

$$\begin{aligned} A' &= A - \frac{\mathrm{Hmono}(A)}{\mathrm{Hmono}(M_i)} M_i \\ &= -\frac{\mathrm{Hmono}(A)}{\mathrm{Hmono}(M_i)} \mathrm{Tail}(M_i) + \mathrm{Tail}(A), \end{aligned}$$

then we say that M_i *reduces* A to A' and we denote this by the expression $A \xrightarrow{M_i} A'$. □

Note that if $A \xrightarrow{M_i} A'$ then

$$A - A' = \frac{\mathrm{Hmono}(A)}{\mathrm{Hmono}(M_i)} M_i = \theta_i M_i \in \mathcal{M}.$$

We should also note that

$$\mathrm{Hterm}(A) \underset{\mathrm{lex}}{\geq} \mathrm{Hterm}(\theta_i M_i), \quad \text{and} \quad \mathrm{Hterm}(A) \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A').$$

We also write $A \xrightarrow{\mathbf{M}} A'$ if $A \xrightarrow{M_i} A'$ for some $M_i \in \mathbf{M}$. Finally, we write $A \xrightarrow[*]{\mathbf{M}} A'$ if

$$A \xrightarrow{\mathbf{M}} A_1 \xrightarrow{\mathbf{M}} \cdots \xrightarrow{\mathbf{M}} A_j \xrightarrow{\mathbf{M}} A',$$

and A' *cannot be reduced any further by* $\mathbf{M}$. Note that the A' obtained by the above process depends on the choice of the M_i's at each step of the reduction. It is thus possible that $A \xrightarrow[*]{\mathbf{M}} A'$, $A \xrightarrow[*]{\mathbf{M}} A''$ and $A' \neq A''$.

Following simple observations are now in order:

1. The length of the sequence of reductions is necessarily finite, since the lexicographic ordering on the head monomials is a well-ordering.
2. We call an irreducible A' obtained from A by a sequence of reductions, as above, a *normal form* of A with respect to $\mathbf{M}$, and is not necessarily unique. We denote the set of normal forms of A by
$$\mathrm{NF}_{\mathbf{M}}(A) = \{A' : A \xrightarrow[*]{\mathbf{M}} A'\} \neq \emptyset.$$
3. It is also evident that $A \xrightarrow[*]{\mathbf{M}} A'$ implies that $A - A' \in \mathcal{M}$, and
$$A = \theta_1 M_1 + \theta_2 M_2 + \cdots + \theta_\nu M_\nu + A',$$
where $\mathrm{Hterm}(A) \underset{\mathrm{lex}}{\geq} \mathrm{Hterm}(\theta_i M_i)$, for all i, and $\mathrm{Hterm}(A) \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A')$.

4. In particular, $A \xrightarrow[*]{\mathbf{M}} 0$ (i.e. $0 \in \mathrm{NF}_{\mathbf{M}}(A)$) implies that $A \in \mathcal{M}$.

Definition 2.3 (Property (E)) A set of generators $\mathbf{M} = \{M_1, M_2, \ldots, M_\nu\}$ of the ideal $\mathcal{M}$ has property (E) if

$$A \in \mathcal{M} \Leftrightarrow A \xrightarrow[*]{\mathbf{M}} 0.$$

In this case, we say that $\mathbf{M}$ is an *E-basis* of the ideal $\mathcal{M}$. □

Note that the property (E) is equivalent to the following seemingly stronger condition:

$$A \in \mathcal{M} \Leftrightarrow \mathrm{NF}_{\mathbf{M}}(A) = \{0\}.$$

If, in fact, our claim were not true then there would be an $A \in \mathcal{M} \setminus \{0\}$, and a choice of reduction sequence such that $A \xrightarrow[*]{\mathbf{M}} A' \neq 0$. But as $A' = A - (A - A') \in \mathcal{M}$, A', itself would be reducible by some $M_i \in \mathbf{M}$.

Thus the property (E) provides an effective procedure to solve ideal membership problem. Assume that the set of generators $\{M_1, \ldots, M_\nu\}$ satisfies the property (E); reduce A with respect to *some* choice of reduction sequence: $A \xrightarrow[*]{\mathbf{M}} A'$, if $A' = 0$ then $A \in \mathcal{M}$; otherwise, $A \notin \mathcal{M}$.

Property (E) is equivalent to property $(E1)$ which says that for every $A \neq 0$ in $\mathcal{M}$, there is an M_i such that $\mathrm{Hmono}(M_i)$ divides $\mathrm{Hmono}(A)$. It is trivial to see that (E) implies $(E1)$; to see the converse, it suffices to observe that $(E1)$ implies that every non-zero $A \in \mathcal{M}$ is reducible.

2.2 Head Monomial Ideal, G-Basis and the Property (SYZ)

Before we present an algorithm to compute an E-basis of an ideal in $\mathbf{Z}[x_1, x_2, \ldots, x_n]$, we relate it to some of the well known concepts, introduced in the context of the computation of a Gröbner bases. We begin with a few definitions:

Definition 2.4 (Head Monomial Ideal) Given a subset $S \subseteq \mathbf{Z}[x_1, x_2, \ldots, x_n]$ we call the ideal generated by all the head monomials of elements in S the *head monomial ideal* of S and denote it $\mathrm{Head}(S)$. □

Note that S is not required to be a finite set. The idea of a Gröbner basis is expressed in these terms by what we shall call property (G).

Definition 2.5 (Property (G)) *A set of generators* $\mathbf{M} = \{M_1, M_2, \ldots, M_\nu\}$ *of the ideal* $\mathcal{M}$ *has property (G) if*

$$\mathrm{Head}(M_1, \ldots, M_\nu) = \mathrm{Head}(\mathcal{M}).[31]$$

In this case, we say that $\mathbf{M}$ *is a G-*basis *of the ideal* $\mathcal{M}$. □

[31] By an abuse of notation, we write $\mathrm{Head}(M_1, \ldots, M_\nu)$, instead of $\mathrm{Head}(\{M_1, \ldots, M_\nu\})$.

Notice that we always have $\mathrm{Head}(M_1, M_2, \ldots, M_\nu) \subseteq \mathrm{Head}(\mathcal{M})$, since $\{M_1, M_2, \ldots, M_\nu\} \subseteq \mathcal{M}$. On the other hand if $\{M_1, M_2, \ldots, M_\nu\}$ has property (E) it follows that it also has property $(E1)$, whence for every $A \in \mathcal{M}$ there is an M_i such that $\mathrm{Hmono}(M_i)$ divides $\mathrm{Hmono}(A)$ and therefore $\mathrm{Hmono}(A) \in \mathrm{Head}(M_1, M_2, \ldots, M_\nu)$ and it follows that $\mathrm{Head}(M_1, M_2, \ldots, M_\nu) = \mathrm{Head}(\mathcal{M})$. Thus property (E) implies property (G). However, the converse is not always true. Consider the following trivial example. Let $\mathcal{M} = (x^2+1)$, $M_1 = 2x^2+2$, $M_2 = 3x^2+3$. Then $\mathcal{M} = (M_1, M_2)$ and

$$\mathrm{Head}(\mathcal{M}) = (x^2) = (2x^2, 3x^2) = \mathrm{Head}(M_1, M_2),$$

and we see that $\{M_1, M_2\}$ has property (G) but it does not have property (E) since x^2+1 is reducible by neither M_1 nor M_2 even though x^2+1 is in $\mathcal{M}$.

Next, we consider the property (SYZ), which is equivalent to property (G) and is a useful aid in the computation.

Definition 2.6 (S-Polynomial) Let M_i and M_j be two distinct polynomials in the ideal $\mathcal{M}$. Then we define the *S-polynomial* of M_i and M_j (denoted, $S(M_i, M_j)$) as follows:

$$S(M_i, M_j) = \frac{\widehat{m}}{\mathrm{Hmono}(M_i)} M_i - \frac{\widehat{m}}{\mathrm{Hmono}(M_j)} M_j,$$

where $\widehat{m} = \mathrm{LCM}\{\mathrm{Hmono}(M_i), \mathrm{Hmono}(M_j)\}$. □

Definition 2.7 (Property (SYZ)) *A set of generators* $\mathrm{M} = \{M_1, \ldots, M_\nu\}$ *of the ideal* $\mathcal{M}$ *has property (SYZ) if for every pair of distinct polynomial* M_i, $M_j \in \mathrm{M}$, $S(M_i, M_j) \in \mathcal{M}$ *can be expressed as*

$$S(M_i, M_j) = \theta_1 M_1 + \cdots + \theta_\mu M_\mu,$$

where $\mathrm{Hterm}(S(M_i, M_j)) \underset{\mathrm{lex}}{\geq} \mathrm{Hterm}(\theta_i M_i)$, *for all i.* □

We recall the following theorem from the Theory of Gröbner Bases[32], without proof.

Theorem 2.1 *Let* $\mathcal{M}$ *be an ideal in* $\mathbf{Z}[x_1, \ldots, x_n]$, *and*

$$\mathrm{M} = \left\{M_1, M_2, \ldots, M_\nu\right\} \subseteq \mathcal{M},$$

a subset of $\mathcal{M}$. *Then the following two statements are equivalent:*

1. $\mathrm{Head}(M_1, M_2, \ldots, M_\nu) = \mathrm{Head}(\mathcal{M})$.
2. $(M_1, M_2, \ldots, M_\nu) = \mathcal{M}$, *and* M *has the property (SYZ).* □

Next consider a more useful, and seemingly weaker condition (SYZ1); a set of generators $\mathrm{M} = \{M_1, \ldots, M_\nu\}$ of the ideal $\mathcal{M}$ has property (SYZ1) if for every pair of distinct polynomial M_i, $M_j \in \mathrm{M}$,

$$S(M_i, M_j) \xrightarrow[*]{\mathrm{M}} 0.$$

[32] *Algorithmic Algebra.*

Obviously, (SYZ1) implies (SYZ), and by the preceding theorem, also the property (G).

Note that if $\{M_1, M_2, \ldots, M_\nu\}$ has property (E) then, since for every pair of distinct polynomials M_i, $M_j \in \mathbf{M}$, $S(M_i, M_j) \in \mathcal{M}$, we have

$$S(M_i, M_j) \xrightarrow[*]{\mathbf{M}} 0,$$

and (E) implies (SYZ1). But, the converse does not always hold. Consider our old example: $\mathcal{M} = (x^2+1)$, $M_1 = 2x^2+2$ and $M_2 = 3x^2+3$. Then $\mathcal{M} = (M_1, M_2)$ and $S(M_1, M_2) = 0$. We conclude that $\{M_1, M_2\}$ has property (SYZ1); but it does not have property (E).

Thus, although we can verify if a set of generators has property (SYZ1) by means of a computable test, such a test is not sufficient for property (E). In some sense, the problem with property (E) is illustrated quite well by the above trivial example, and can be fixed equally trivially, using the following machinery.

2.3 The Ψ Expansion

Let $\mathcal{M}$ be an ideal and $\mathbf{M} = \{M_1, M_2, \ldots, M_\nu\}$ be a subset of polynomials in $\mathbf{Z}[x_1, x_2, \ldots, x_n]$. For every non-empty subset $\mathbf{M}' = \{M_{i_1}, \ldots, M_{i_\mu}\} \subseteq \mathbf{M}$, we let

$$\begin{aligned} q &= \gcd\Big\{\mathrm{Hcoef}(M_{i_1}), \ldots, \mathrm{Hcoef}(M_{i_\mu})\Big\} \\ &= a_1 \mathrm{Hcoef}(M_{i_1}) + \cdots + a_\mu \mathrm{Hcoef}(M_{i_\mu}), \end{aligned}$$

where q, $a_1, \ldots, a_\mu \in \mathbf{Z}$, and we let,

$$\pi = \mathrm{LCM}\Big\{\mathrm{Hterm}(M_{i_1}), \ldots, \mathrm{Hterm}(M_{i_\mu})\Big\}$$

whence,

$$q \cdot \pi = a_1 \frac{\pi}{\mathrm{Hterm}(M_{i_1})} \mathrm{Hmono}(M_{i_1}) + \cdots + a_\mu \frac{\pi}{\mathrm{Hterm}(M_{i_\mu})} \mathrm{Hmono}(M_{i_\mu})$$

and clearly $q \cdot \pi \in \mathrm{Head}(M_1, \ldots, M_\nu)$. Thus, for every such $\mathbf{M}'$ we define

$$\psi(\mathbf{M}') = a_1 \frac{\pi}{\mathrm{Hterm}(M_{i_1})} M_{i_1} + \cdots + a_\mu \frac{\pi}{\mathrm{Hterm}(M_{i_\mu})} M_{i_\mu}.$$

Clearly, $\psi(\mathbf{M}') \in (M_1, \ldots, M_\nu)$ and $\mathrm{Hmono}(\psi(\mathbf{M}')) = q \cdot \pi \in \mathrm{Head}(M_1, \ldots, M_\nu)$. This leads us to define the Ψ expansion of $\mathbf{M}$ to be

$$\begin{aligned} \Psi(\mathbf{M}) &= \Psi\Big(\{M_1, \ldots, M_\nu\}\Big) \\ &= \Big\{M_1, \ldots, M_\nu\Big\} \bigcup \Big\{\psi(\mathbf{M}') : \emptyset \subsetneq \mathbf{M}' \subseteq \mathbf{M} \\ &\qquad \& \ (\forall 1 \le i \le \nu)\ [\mathrm{Hmono}(M_i) \text{ does not divide } \mathrm{Hmono}(\psi(\mathbf{M}'))]\Big\} \\ &= \{P_1, \ldots, P_\lambda\} = \mathbf{P}, \end{aligned}$$

where we have removed duplicates or multiples with respect to the head monomials. Moreover, it is clear that

$$\begin{aligned} \mathrm{Head}(M_1, \ldots, M_\nu) &= \mathrm{Head}(P_1, \ldots, P_\lambda), \text{ and} \\ (M_1, \ldots, M_\nu) &= (P_1, \ldots, P_\lambda). \end{aligned}$$

Definition 2.8 (Property (Ψ)) A set $\{M_1, \ldots, M_\nu\}$ has property (Ψ) if it is closed under the Ψ expansion, i.e.

$$\Psi(\mathrm{M}) = \mathrm{M}. \quad \square$$

Lemma 2.2 *Let* $\mathrm{M} = \{M_1, \ldots, M_\nu\}$ *be a set of generators of* $\mathcal{M}$. *If the set* M *satisfies the property (E) then it also satisfies the property (Ψ).*

PROOF.

Assume to the contrary, i.e. M satisfies property (E) but not (Ψ). Then there is an element $A \in \Psi(\mathrm{M}) \setminus \mathrm{M} \subseteq \mathcal{M}$ such that Hmono(A) is not divisible by any Hmono(M_i), where $M_i \in \mathrm{M}$. But then this directly contradicts the property ($E1$). $\square$

We note that $\Psi(\mathrm{M})$ has property (Ψ), regardless of what M is considered, since $\Psi(\Psi(\mathrm{M})) = \Psi(\mathrm{M})$[33]. We also remark that if the set M is finite then its expansion is finite, and effectively constructible (via Euclid's Algorithm; see appendix 1).

2.4 Characterization of an E-Basis

Theorem 2.3 *Let* $\mathrm{M} = \{M_1, \ldots, M_\nu\}$ *be a set of generators of* $\mathcal{M}$.

1. *If* M *satisfies the property (G) then* $\Psi(\mathrm{M})$ *is a set of generators of* $\mathcal{M}$ *satisfying the property (E).*
2. *If* M *satisfies the property* (SYZ1) *then* $\Psi(\mathrm{M})$ *is a set of generators of* $\mathcal{M}$ *satisfying the property (E).*

PROOF.

[33] Note that

$$(\forall \emptyset \subsetneq \mathrm{P}' \subseteq \Psi(\mathrm{M}))\, (\exists \mathrm{M}' \subseteq \mathrm{M})\, [\mathrm{Hmono}(\psi(\mathrm{P}')) = \mathrm{Hmono}(\psi(\mathrm{M}'))].$$

A suitable choice for M′ is as follows:

$$\mathrm{M}' = \Big(\mathrm{P}' \cap \mathrm{M}\Big) \cup \bigcup \Big\{\mathrm{M}'' : \psi(\mathrm{M}'') \in \mathrm{P}' \setminus \mathrm{M}\Big\}.$$

Thus,

$$\begin{aligned} \mathrm{Hcoef}(\psi(\mathrm{M}')) &= \mathrm{Hcoef}(\psi(\mathrm{P}')) \quad \text{and} \\ \mathrm{Hterm}(\psi(\mathrm{M}')) &= \mathrm{Hterm}(\psi(\mathrm{P}')), \end{aligned}$$

i.e. $\mathrm{Hmono}(\psi(\mathrm{M}')) = \mathrm{Hmono}(\psi(\mathrm{P}'))$. Hence,

$$\begin{aligned} \Psi(\Psi(\mathrm{M})) \setminus \Psi(\mathrm{M}) &= \Big\{\psi(\mathrm{P}') : \emptyset \subsetneq \mathrm{P}' \subseteq \Psi(\mathrm{M}) \\ &\qquad (\forall \mathrm{M}' \subseteq \mathrm{M})\, [\mathrm{Hmono}(\psi(\mathrm{M}')) \text{ does not divide } \mathrm{Hmono}(\psi(\mathrm{P}'))]\Big\} \\ &= \emptyset. \end{aligned}$$

$$\begin{tikzcd}
 & & (E) \arrow[r, leftrightarrow] \arrow[dll] \arrow[dd] \arrow[ddr] & (E1) \\
(\textsc{syz}1) \arrow[dr] & & & \\
 & (\textsc{syz}) \arrow[r, Leftrightarrow] & (G) & (\Psi)
\end{tikzcd}$$

$$\begin{tikzcd}
(G) \mathbin{\&} (\Psi) \arrow[dr] & & (\textsc{syz}1) \mathbin{\&} (\Psi) \arrow[dl] \\
 & (E) &
\end{tikzcd}$$

Figure 1: RELATIONS AMONG THE PROPERTIES.

(1) Since $\mathrm{M} \subseteq \Psi(\mathrm{M}) \subseteq \mathcal{M}$, evidently, $\Psi(\mathrm{M})$ is a set of generators of $\mathcal{M}$. Let $A \in \mathcal{M}$. As M satisfies property (G), it follows that $\mathrm{Hmono}(A) \in \mathrm{Head}(M_1, \ldots, M_\nu)$, and it can be expressed as follows:

$$\begin{aligned}
\mathrm{Hmono}(A) &= a_1\pi_1\mathrm{Hmono}(M_{i_1}) + \cdots + a_\mu\pi_\mu\mathrm{Hmono}(M_{i_\mu}) \\
&\qquad \text{where } a_j \in \mathbf{Z} \setminus \{0\} \;\&\; \mathrm{Hterm}(A) = \pi_j\mathrm{Hterm}(M_{i_j}) \\
&= \Big[a_1\mathrm{Hcoef}(M_{i_1}) + \cdots + a_\mu\mathrm{Hcoef}(M_{i_\mu})\Big] \cdot \\
&\qquad \pi' \cdot \mathrm{LCM}\Big\{\mathrm{Hterm}(M_{i_1}), \ldots, \mathrm{Hterm}(M_{i_\mu})\Big\} \\
&= (q' \cdot q)(\pi' \cdot \pi).
\end{aligned}$$

Now, if we consider the subset $\mathrm{M}' = \{M_{i_1}, \ldots, M_{i_\mu}\}$, then $\mathrm{Hmono}(\psi(\mathrm{M}')) = q \cdot \pi$, and thus there must be a polynomial in $\Psi(\mathrm{M})$, whose head monomial divides $\mathrm{Hmono}(A)$.

(2) This is an immediate consequence of the fact that the property (SYZ1) implies (G). □

Corollary 2.4 *Let* $\mathrm{M} = \{M_1, \ldots, M_\nu\}$ *be a set of generators of* $\mathcal{M}$. *Then*

1. *The set* M *satisfies the properties* (G) *and* (Ψ) *if and only if it satisfies the property* (E).

2. *The set* M *satisfies the properties* (SYZ1) *and* (Ψ) *if and only if it satisfies the property* (*E*).

PROOF.
Both the assertions follow from the previous theorem and the facts that (E) implies (G), (SYZ1) and (Ψ) (see lemma 2.2 and the related remarks). □

2.5 The Algorithm

Now, we are ready to present our algorithm to compute an E-basis for an ideal. Recall, from the discussion earlier, that this would provide us with an effective procedure to decide the ideal membership problem:

```
E-Basis Algorithm:

Input:   $\mathbf{M} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$,
         $\mathbf{M}$ = finite.
Output:  $\mathbf{P} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$,
         $(\mathbf{P}) = (\mathbf{M})$, and $\mathbf{P}$ satisfies the property $(E)$.

    $\mathbf{P} := \mathbf{M}$;  $\mathbf{P} := \Psi(\mathbf{P})$;
    Pairs := $\{\{M_i, M_j\} : M_i, M_j \in \mathbf{P}$ & $M_i \neq M_j\}$;

    while Pairs $\neq \emptyset$ loop
        Choose $\{M_i, M_j\}$, any pair in Pairs;
        Pairs := Pairs $\setminus \{\{M_i, M_j\}\}$;
        Compute a normal form $P$ of $S(M_i, M_j)$ with respect to some
            choice of sequence of reductions modulo $\mathbf{P}$;
        $P = \mathrm{NF}_{\mathbf{P}}(S(M_i, M_j))$;
        if $P \neq 0$ then
            $\mathbf{P} := \mathbf{P} \cup \{P\}$;  $\mathbf{P} := \Psi(\mathbf{P})$;
            Pairs := $\{\{M_i, M_j\} : M_i, M_j \in \mathbf{P}$ & $M_i \neq M_j\}$;
        end if ;
    end loop ;
    return $\mathbf{P}$;
end E-Basis Algorithm.   □
```

Consider a sequence of values assumed by the variable $\mathbf{P}$ during an execution of the E-Basis Algorithm, say $\mathbf{P}_1 = \mathbf{M}$, $\mathbf{P}_2$, $\mathbf{P}_3$, …, $\mathbf{P}_{2N'-1}$, $\mathbf{P}_{2N'} = \mathbf{P}$, (if we may assume that the algorithm terminates), where:

1. $\mathbf{P}_{2i} = \Psi(\mathbf{P}_{2i-1})$, $(i = 1, \ldots, N')$, and

2. $\mathbf{P}_{2i+1} = \mathbf{P}_{2i} \cup \{P_{2i}\}$ $(i = 1, \ldots, N'-1)$, $P_{2i} \in (\mathbf{P}_{2i})$, and P_{2i} is not reducible with respect to $\mathbf{P}_{2i}$.

We make the following observations:

- For $i = 1, \ldots, N'$, $(\mathbf{P}_{2i}) = (\mathbf{P}_{2i-1})$, (see the discussion in the subsection 2.3). For $i = 1$, …, $N' - 1$, $(\mathbf{P}_{2i+1}) = (\mathbf{P}_{2i})$, since $P_{2i} \in (\mathbf{P}_{2i})$. Thus, $(\mathbf{P}) = (\mathbf{M})$.

- Clearly, $\mathbf{P}_{2N'} = \mathbf{P}$ satisfies the property (SYZ1) (otherwise, it would violate the assumption that the algorithm terminates). Thus, by theorem 2.3, $\Psi(\mathbf{P})$ satisfies the property (E). But, since $\mathbf{P} = \mathbf{P}_{2N'} = \Psi(\mathbf{P}_{2N'-1})$, we have
$$\Psi(\mathbf{P}) = \Psi(\Psi(\mathbf{P}_{2N'-1})) = \Psi(\mathbf{P}_{2N'-1}) = \mathbf{P},$$
and $\mathbf{P}$ itself satisfies property (E).

In summary:

Theorem 2.5 (Weak Correctness of the E-Basis Algorithm**)** *Given a finite set* $\mathbf{M} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$, *the algorithm* E-Basis Algorithm *correctly produces an* E*-basis of the ideal* $\mathcal{M} = (\mathbf{M})$, *when it terminates.* □

Thus, for our purpose, it suffices to show that the algorithm terminates after some finite number N steps. The following observation will be useful in the subsequent arguments:

Note for all $i = 1, \ldots, N' - 1$, $\text{Hmono}(P_{2i})$ is not divisible by the $\text{Hmono}(M_j)$'s, for all $M_j \in \mathbf{P}_{2i}$. Thus $\text{Hmono}(P_{2i}) \notin \text{Head}(\mathbf{P}_{2i-1})$, since otherwise by the arguments in subsection 2.3 $\text{Hmono}(P_{2i})$ would be divisible by the head monomial of some polynomial in $\Psi(\mathbf{P}_{2i-1}) = \mathbf{P}_{2i}$. Thus, for all $i = 1, \ldots,$
$$\text{Head}(\mathbf{P}_{2i-1}) \subsetneq \text{Head}(\mathbf{P}_{2i+1}).$$

Thus, if we can show that such an ascending chain of monomial ideals is of some bounded length[34] then we can obtain an upper bound on the number of steps the algorithm takes before termination.

It is well known that given an arbitrary ascending chain of monomial ideals it is not possible to bound the length of the chain simply by the size of the basis for the first ideal; for example, the following ascending chain of monomial ideals can be of arbitrary length, depending on the parameter P and independent of the size of the basis for the first monomial ideal:
$$(x^2y^2) \subsetneq (xy^P) \subsetneq (xy^{P-1}) \subsetneq (xy^{P-2}) \subsetneq \cdots$$

However, we can circumvent this problem, since we have additional informations on the sizes of the bases of all the monomial ideals in the chain.

Using the bounds from the appendices 1 and 2, we see that, if we know that $\text{Head}(\mathbf{P}_{2i-1})$ has a monomial basis with coefficients and degrees bounded respectively by C and D, then $\text{Head}(\mathbf{P}_{2i+1})$ has a monomial basis, whose coefficients and degrees are bounded respectively by
$$\begin{aligned} \left(C^C\right)^{2+3^n(D+1)^{n(n+1)/2}} &\leq 2^{2^{2^{2^{\max\{C,D,n\}}}}}, \quad \text{and} \\ 2(2D+1)^N &\leq 2^{2^{2^{\max\{C,D,n\}}}}. \end{aligned}$$

Also, if $\text{Head}(\mathbf{P}_{2i-1})$ has a monomial basis with λ generators then $\text{Head}(\mathbf{P}_{2i+1})$ has a monomial basis with at most 2^λ generators.

[34] Since $\mathbb{Z}$ is Noetherian, by Hilbert's Ascending Chain Condition, one can show that such a chain of ideals must be of finite length. However, this argument is non-constructive in nature and suffers from the problem alluded to in the introductory section.

Later on in the paper we shall use the following notation:

$$2 \uparrow^{(i)} (x) \quad \text{to denote} \quad \left. 2^{2^{\cdot^{\cdot^{2^x}}}} \right\} i,$$

and call it the i^{th} *tower function*. We also write $2 \uparrow^{(i)}$ for $2 \uparrow^{(i)} (1)$.

Thus, we see that, if we start with a system of ν polynomials with coefficients and degrees bounded by c and d respectively, then the monomial ideal $\text{Head}(\mathbf{P}_{2i+1})$ has a basis with consisting of at most $2 \uparrow^{(i)} (\nu)$ elements whose degrees and coefficients are both bounded by

$$2 \uparrow^{(5i)} (\max\{c, d, n\}) \leq 2 \uparrow^{(5i+\max\{c,d,n\})} .$$

In particular,

Theorem 2.6 *Let N' bound the length of any ascending chain of monomial ideals*

$$\mathcal{M}_1 \subsetneq \mathcal{M}_2 \subsetneq \cdots \subsetneq \mathcal{M}_i \subsetneq \cdots,$$

where $\mathcal{M}_i$ has a monomial basis with coefficients and degrees bound of $2 \uparrow^{(5i+\max\{c,d,n\})}$. Then our algorithm to compute an E-basis of a set of ν polynomials $\mathbf{M} \subseteq \mathbf{Z}[x_1, \ldots, x_n]$ of coefficients and degrees bounds of c and d, respectively, uses no more than N arithmetic steps, where

$$N \leq 2 \uparrow^{(5(N'+1)+\max\{\nu,c,d,n\})} . \quad \square$$

Henceforth we shall concentrate on obtaining the bound N' for the length of an ascending chain of monomial ideals satisfying the conditions of the preceding theorem. In fact, we will do little more: Consider an ascending chain of monomial ideals

$$\mathcal{M}_1 \subsetneq \mathcal{M}_2 \subsetneq \cdots \subsetneq \mathcal{M}_i \subsetneq \cdots,$$

where $\mathcal{M}_i$ has a monomial basis with coefficients and degrees bound of $f(i + \kappa)$ and f is a monotonically increasing function; we shall derive a bound on the length of the chain of ideals. Of course, the bound we derive will depend on the function f. From such a general bound, obtaining the bounds N and N' is a trivial matter, once we identify f with the function $2 \uparrow^{(5i+\max\{c,d,n\})}$. However, the bounds we shall derive are going to be rather crude and will be given in terms of a class of rapidly growing (but primitive recursive) functions. In the following two sections, we shall develop the necessary tools.

3. Rapidly Growing Functions

In this section, we start with an explicit description of certain provably recursive functions due to S.S. Wainer[35]. The Wainer characterization itself can be derived from a previous characterization due to Kreisel in terms ordinal recursion of order $< \varepsilon_0$, and has lately found many applications in logic, e.g. Paris-Harrington Theorem[36] (a variant of Finite Ramsey Theorem) and Friedman's Finite Form (FFF) of Krushkal's Theorem. However, for our purpose, we only need the initial primitive recursive segment of a slight variant of the Wainer Hierarchy, which we describe below.

Definition 3.9 (Wainer Hierarchy) Let $\{F_\alpha\}$ $(0 \leq \alpha \leq \varepsilon_0)$ be a family of functions, defined as follows:

$$\begin{aligned} F_0(x) &= x+1 \\ F_{\alpha+1}(x) &= F_\alpha^{(x+1)}(x), \quad \text{if } \alpha \text{ is a successor ordinal;} \\ & \quad (G^{(m)}\text{is the } m\text{-fold application of } G) \\ F_\alpha(x) &= \max_{k \leq x}(F_{j_k}(x)), \quad \text{if } \alpha \text{ is a limit ordinal.} \\ & \quad (j_k \text{ is the } k^{\text{th}} \text{ element in a canonical fundamental sequence} \\ & \qquad \text{converging to } \alpha.) \quad \square \end{aligned}$$

Thus at each successive stage, we obtain the next rapidly growing function by diagonalizing over the current function by x-fold applications, and at limits, we obtain a more rapidly growing function by diagonalizing over the family of functions indexed by the elements of a sequence converging to the limit. It can be shown that these functions are all monotonically increasing and that F_β is more rapidly growing than F_α if and only if $\alpha < \beta$. It can also be shown that F_1, F_2, F_3, etc. are all primitive recursive and that F_ω has the same order of growth as Ackermann's function. (Thus F_ω is an example of a recursive function that is not primitive recursive.)

Definition 3.10 Consider a monotonically increasing function[37] $f\colon \mathbf{N} \to \mathbf{N}$. f is said to be in W_n (i.e. in the n^{th} level of Wainer hierarchy, if $f(x) \leq F_n(x)$ almost everywhere (i.e. for all but finitely many x). □

Example: The first few functions have the following approximate order of growth:

$$\begin{aligned} F_0(x) &= x+1 \\ F_1(x) &\approx 2x \\ F_2(x) &\approx 2^x \\ F_3(x) &\approx 2 \uparrow^{(x)} (x) \end{aligned}$$

[35] S.S. Wainer. *A Classification of the Ordinal Recursive Functions*, *Arch. Math. Logik*, **13**, (1970), pp. 136–153. J. Keaton and R. Solovay. *Rapidly Growing Ramsey Functions*, *Unpublished Manuscript*, (1980).

[36] Jeff Paris and Leo Harrington. *A Mathematical Incompleteness in Peano Arithmetic*, *Handbook of Mathematical Logic:* (Edited by Jon Barwise), (1977), pp. 1133–1142.

[37] Since we are only interested in the "rate of growth" of the functions, there is no harm in assuming that f is monotonically increasing.

These approximate equalities are quite "tight;" for instance, for x sufficiently large ,

$$2 \uparrow^{(x+1)} (x) \leq F_3(x) \leq 2 \uparrow^{(x+2)} (x).$$

We now state a few elementary facts about Wainer hierarchy. Let f, g and h be monotonically increasing functions.

Fact 1:

$$g \in W_i \quad \Rightarrow \quad g \in W_{i+k}, \qquad \text{for all } k \in \mathbb{N}.$$

Thus, a function in the i^{th} level of the hierarchy is also in the higher levels of the hierarchy.

Fact 2:

$$g, h \in W_i \quad \Rightarrow \quad g + h \in W_{i+1} \text{ and } g \cdot h \in W_{i+1}.$$

In general, any arithmetic combination of a finite (fixed) number of functions in the i^{th} level of the hierarchy is in the next level of the hierarchy.

Fact 3: Let $f \in W_i$ $(i > 1)$. Let g be a function defined recursively in terms of f as follows:

$$\begin{aligned} g(0) &= k, \quad k = \text{a constant} \\ g(x) &= f(g(x-1)), \quad \text{if } x > 0. \end{aligned}$$

Then $g \in W_{i+1}$.

Note that, for x sufficiently large

$$g(x) = f^{(x)}(k) \leq f^{(x)}(x) \leq F_i^{(x)}(x) \leq F_i^{(x+1)}(x) = F_{i+1}(x).$$

Fact 4:

$$g, h \in W_i \quad \Rightarrow \quad g \circ h \in W_{i+1},$$

where $\circ$ denotes functional composition.

Note that, for x sufficiently large

$$g(h(x)) \leq g(F_i(x)) \leq F_i^{(2)}(x) \leq F_i^{(x+1)}(x) \leq F_{i+1}(x).$$

In general, any functional composition of a finite (fixed) number of functions in the i^{th} level of the hierarchy is in the next level of the hierarchy.

In particular, if $g \in W_i$ $(i > 1)$ then $2^g \in W_{i+1}$ and $2 \uparrow^{(k)} g \in W_{i+1}$, assuming k is a fixed constant.

4. Ascending Chain of Monomial Ideals

In order to prove the required bounds, we start with some simple algebraic preliminaries. Our proof techniques will be closely based on a technique, first used by A. Seidenberg[38].

We start by considering the following rings of multivariate polynomials over the integers and rationals:

$$\begin{aligned} &\mathbf{Q}[x_1,\ldots,x_n], \\ \mathbf{Q}[x_1,\ldots,\widehat{x_j},\ldots,x_n] &= \mathbf{Q}[x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n], \\ \mathbf{Z}[x_1,\ldots,x_n] &\text{ and} \\ \mathbf{Z}[x_1,\ldots,\widehat{x_j},\ldots,x_n] &= \mathbf{Z}[x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n]. \end{aligned}$$

Note that, in our notation $x_1, \ldots, \widehat{x_j}, \ldots, x_n$ stand for the sequence of variables from x_1 through x_n with the variable x_j missing.

First, we consider the following ring homomorphisms (projections):

$$\begin{aligned} \Pi_0 &: \mathbf{Z}[x_1,\ldots,x_n] \to \mathbf{Q}[x_1,\ldots,x_n] \\ &: f(x_1,\ldots,x_n) \mapsto f(x_1,\ldots,x_n), \\ \Pi_j &: \mathbf{Z}[x_1,\ldots,x_n] \to \mathbf{Z}[x_1,\ldots,x_n]/(x_j-1) \cong \mathbf{Z}[x_1,\ldots,\widehat{x_j},\ldots,x_n] \\ &: f(x_1,\ldots,x_n) \mapsto f(x_1,\ldots,x_n)_{x_j=1}, \\ &\quad 1 \le j \le n. \end{aligned}$$

Now, if $\mathcal{M} \subseteq \mathbf{Z}[x_1,\ldots,x_n]$ is an ideal then we define

$$\mathcal{M}^{(j)} = (\Pi_j(\mathcal{M}))^e$$

as the extension ideal of $\mathcal{M}$ with respect to the homomorphism Π_j. Thus, this is the ideal generated by $\{\Pi_j(f) : f \in \mathcal{M}$ in the ring = Range Π_j.

We note that if $\mathcal{M}_i$ and $\mathcal{M}_{i+1} \subseteq \mathbf{Z}[x_1,\ldots,x_n]$ are two ideals such that $\mathcal{M}_i \subseteq \mathcal{M}_{i+1}$ then

$$\mathcal{M}_i^{(0)} \subseteq \mathcal{M}_{i+1}^{(0)}, \quad \mathcal{M}_i^{(1)} \subseteq \mathcal{M}_{i+1}^{(1)}, \quad \ldots, \mathcal{M}_i^{(n)} \subseteq \mathcal{M}_{i+1}^{(n)}.$$

The following technical lemma and its variants will play a crucial in the rest of the paper.

Lemma 4.7 (Main Technical Lemma)
Assume that $\mathcal{M}_i$ and $\mathcal{M}_{i+1}$ are two monomial ideals in $\mathbf{Z}[x_1, \ldots, x_n]$, where the ideals have monomial bases with sizes (i.e. coefficients and exponents in each variable) bounded by the function values $f(i+\kappa)$ and $f(i+1+\kappa)$, $f(i+\kappa) \le f(i+1+\kappa)$.

Further, assume that $\mathcal{M}_i \subsetneq \mathcal{M}_{i+1}$, but

$$\mathcal{M}_i^{(0)} = \mathcal{M}_{i+1}^{(0)}, \quad \mathcal{M}_i^{(1)} = \mathcal{M}_{i+1}^{(1)}, \quad ,\ldots, \quad \mathcal{M}_i^{(n)} = \mathcal{M}_{i+1}^{(n)}.$$

[38] A. Seidenberg. *An Elimination Theory for Differential Algebra, Univ. of Califorina Pub. in Math. New series,* Univ. of Cal. Press, Berkeley and Los Angeles, 3:2 (1956), pp. 31–66.

Let M *denote a minimal monomial basis of* $\mathcal{M}$. *Then* $\mathcal{M}_{i+1}$ *has a monomial basis containing* M$_i$ *and with sizes bounded by* $f(i+\kappa)$.

PROOF.

Let

$$\mathrm{M}_i = \left\{ \begin{array}{l} b_1\, x_1^{r_{11}} \cdots x_j^{r_{1j}} \cdots x_n^{r_{1n}}, \\ \ldots, \\ b_i\, x_1^{r_{i1}} \cdots x_j^{r_{ij}} \cdots x_n^{r_{in}}, \\ \ldots, \\ b_\ell\, x_1^{r_{\ell 1}} \cdots x_j^{r_{\ell j}} \cdots x_n^{r_{\ell n}} \end{array} \right\}$$

be a finite monomial basis of $\mathcal{M}_i$. (The finiteness follows from the bounds on sizes: b_i, $r_{ij} \le f(i+\kappa)$.) Without loss of generality, we may assume that all the b_i's are positive. Also note that

$$\left\{ x_1^{r_{11}} \cdots x_j^{r_{1j}} \cdots x_n^{r_{1n}},\ \ldots,\ x_1^{r_{i1}} \cdots x_j^{r_{ij}} \cdots x_n^{r_{in}},\ \ldots,\ x_1^{r_{\ell 1}} \cdots x_j^{r_{\ell j}} \cdots x_n^{r_{\ell n}} \right\}$$

is a basis for $\mathcal{M}_i^{(0)}$ and

$$\Big\{ b_1\, x_1^{r_{11}} \cdots x_{j-1}^{r_{1(j-1)}}\, x_{j+1}^{r_{1(j+1)}} \cdots x_n^{r_{1n}},\ \ldots,$$
$$b_i\, x_1^{r_{i1}} \cdots x_{j-1}^{r_{i(j-1)}}\, x_{j+1}^{r_{i(j+1)}} \cdots x_n^{r_{in}},\ \ldots,\ b_\ell x_1^{r_{\ell 1}} \cdots x_{j-1}^{r_{\ell(j-1)}}\, x_{j+1}^{r_{\ell(j+1)}} \cdots x_n^{r_{\ell n}} \Big\}$$

is a basis for $\mathcal{M}_i^{(j)}$.

Let M$'_{i+1}$ be a minimal monomial basis of $\mathcal{M}_{i+1}$ containing M$_i$. Such a basis exists since M$_i \cup$ M$_{i+1}$ is a basis of $\mathcal{M}_{i+1}$ containing M$_i$. Let $a\, x_1^{p_1} \cdots x_j^{p_j} \cdots x_n^{p_n}$ be a monomial in M$'_{i+1}$ but not $\mathcal{M}_i$. (Again assume that $a > 0$.)

First, assume to the contrary, i.e. $p_j > f(i+\kappa)$. Then

$$a\, x_1^{p_1} \cdots x_{j-1}^{p_{j-1}}\, x_{j+1}^{p_{j+1}} \cdots x_n^{p_n} \in \mathcal{M}_{i+1}^{(j)} = \mathcal{M}_i^{(j)}.$$

Thus, we can express the monomial $a\, x_1^{p_1} \cdots x_{j-1}^{p_{j-1}}\, x_{j+1}^{p_{j+1}} \cdots x_n^{p_n}$ as a linear combination of the elements of the basis of $\mathcal{M}_i^{(j)}$:

$$\begin{aligned} & a\, x_1^{p_1} \cdots x_{j-1}^{p_{j-1}}\, x_{j+1}^{p_{j+1}} \cdots x_n^{p_n} \\ &= \sum_{i=1}^{\ell} g_i(x_1, \ldots, x_{j-1}, x_{j+1} \ldots, x_n) \cdot b_i\, x_1^{r_{i1}} \cdots x_{j-1}^{r_{i(j-1)}}\, x_{j+1}^{r_{i(j+1)}} \cdots x_n^{r_{in}}, \end{aligned}$$

where $g_i \in \mathbf{Z}[x_1, \ldots, \widehat{x_j}, \ldots, x_n]$. But since $r_{ij} \le f(i+\kappa)$, $p_j > r_{ij}$ and we can express the monomial $a\, x_1^{p_1} \cdots x_j^{p_j} \cdots x_n^{p_n}$ as a linear combinations of the elements of M$_i$:

$$\begin{aligned} & a\, x_1^{p_1} \cdots x_j^{p_j} \cdots x_n^{p_n} \\ &= \sum_{i=1}^{\ell} g_i(x_1, \ldots, x_{j-1}, x_{j+1} \ldots, x_n) \cdot x_j^{p_j - r_{ij}} \cdot b_i\, x_1^{r_{i1}} \cdots x_{j-1}^{r_{i(j-1)}}\, x_j^{r_{ij}} x_{j+1}^{r_{i(j+1)}} \cdots x_n^{r_{in}}, \end{aligned}$$

thus contradicting the hypothesis that $a\, x_1^{p_1} \cdots x_j^{p_j} \cdots x_n^{p_n} \not\in \mathcal{M}_i$.

Now assume that $a > f(i+\kappa)$. Then

$$x_1^{p_1} \cdots x_n^{p_n} \in \mathcal{M}_{i+1}^{(0)} = \mathcal{M}_i^{(0)}.$$

Hence, M_i contains an element of the form

$$b_i\, x_1^{r_{i1}} \cdots x_n^{r_{in}},$$

such that $b_i < a$ (since $b_i \le f(i+\kappa)$), $r_{i1} \le p_1, \ldots, r_{in} \le p_n$ and a is not divisible by b_i. Let M''_{i+1} be a new set of monomials obtained from M'_{i+1} after replacing the monomial $a\, x_1^{p_1} \cdots x_n^{p_n}$ by

$$\begin{aligned}&(a - b_i)\, x_1^{p_1} \cdots x_n^{p_n}\\ &\quad = \; a\, x_1^{p_1} \cdots x_n^{p_n} - x_1^{p_1 - r_{i1}} \cdots x_n^{p_n - r_{in}} (b_i\, x_1^{r_{i1}} \cdots x_n^{r_{in}}).\end{aligned}$$

But this yields a monomial basis M''_{i+1} of $\mathcal{M}_{i+1}$ containing M_i which contradicts the minimality of M'_i. This completes the proof of the lemma. □

Corollary 4.8 *Assume that*

$$\mathcal{M}_i \subsetneq \mathcal{M}_{i+1} \subsetneq \cdots \subsetneq \mathcal{M}_{k-1} \subsetneq \mathcal{M}_k \subsetneq \cdots \subsetneq \mathcal{M}_\ell$$

is an ascending chain of monomial ideals in $\mathbf{Z}[x_1, \ldots, x_n]$, *with monomial bases of sizes bounded by the function values:*

$$f(i+\kappa) \le f(i+1+\kappa) \le \cdots \le f(k-1+\kappa) \le f(k+\kappa) \le \cdots \le f(\ell+\kappa).$$

Further assume that for all $0 \le j \le n$,

$$\mathcal{M}_i^{(j)} = \mathcal{M}_{i+1}^{(j)} = \cdots = \mathcal{M}_{k-1}^{(j)} = \mathcal{M}_k^{(j)} = \cdots = \mathcal{M}_\ell^{(j)}.$$

Then there is a monomial in $\mathrm{M}_k \setminus \mathrm{M}_{k-1}$ *whose sizes are bounded by* $f(i+\kappa)$. *Thus*

$$\ell \le i + [f(i+\kappa)+1]^{n+1}.$$

PROOF.

First note that $\mathcal{M}_k$ has a monomial basis M_k such that

$$\mathrm{M}_k \supseteq \mathrm{M}_{k-1} \supseteq \cdots \supseteq \mathrm{M}_i,$$

and $\mathcal{M}_k \supsetneq \mathcal{M}_i$ and for all $0 \le j \le n$

$$\mathcal{M}_k^{(j)} = \mathcal{M}_i^{(j)}.$$

By the previous lemma, $\mathcal{M}_k$ has a monomial basis M_k whose sizes are bounded by $f(i+\kappa)$. In particular,

$$\Big(\exists \text{ monomials } m_{i+1}, \ldots, m_k, \ldots, m_\ell\Big)$$
$$\Big[m_k \in \mathrm{M}_k \setminus \mathrm{M}_{k-1} \text{ and } |m_k| \le f(i+\kappa)\Big].$$

Thus we can always find $(\ell - i)$ distinct monomials whose sizes are bounded by $f(i+\kappa)$. But then the number of such monomials (i.e. $[f(i+\kappa)+1]^{n+1}$) provides a simple upper bound on $\ell - i$. □

Now, proceeding in a manner similar to the one outlined in this section, and only considering the ring homomorphisms

$$\begin{aligned} \Pi'_j &: \mathbb{Q}[x_1,\ldots,x_n] \to \mathbb{Q}[x_1,\ldots,x_n]/(x_j-1) \cong \mathbb{Q}[x_1,\ldots,\widehat{x_j},\ldots,x_n] \\ &: f(x_1,\ldots,x_n) \mapsto f(x_1,\ldots,x_n)_{x_j=1}, \qquad 1 \le j \le n, \end{aligned}$$

we can also prove the following:

Corollary 4.9 *Assume that*

$$\mathcal{M}_i \subsetneq \mathcal{M}_{i+1} \subsetneq \cdots \subsetneq \mathcal{M}_{k-1} \subsetneq \mathcal{M}_k \subsetneq \cdots \subsetneq \mathcal{M}_\ell$$

is an ascending chain of monomial ideals in $\mathbb{Q}[x_1, \ldots, x_n]$, with monomial bases of sizes bounded by the function values:

$$f(i+\kappa) \le f(i+1+\kappa) \le \cdots \le f(k-1+\kappa) \le f(k+\kappa) \le \cdots \le f(\ell+\kappa).$$

Further assume that for all $1 \le j \le n$,

$$\mathcal{M}_i^{(j)} = \mathcal{M}_{i+1}^{(j)} = \cdots = \mathcal{M}_{k-1}^{(j)} = \mathcal{M}_k^{(j)} = \cdots = \mathcal{M}_\ell^{(j)}.$$

Then there is a monomial in $\mathbf{M}_k \setminus \mathbf{M}_{k-1}$ whose sizes are bounded by $f(i+\kappa)$. Thus

$$\ell \le i + [f(i+\kappa)+1]^n. \quad \square$$

Lemma 4.10 *Assume that*

$$\mathcal{M}_i \subsetneq \mathcal{M}_{i+1} \subsetneq \cdots \subsetneq \mathcal{M}_{k-1} \subsetneq \mathcal{M}_k \subsetneq \cdots \subsetneq \mathcal{M}_\ell$$

is an ascending chain of ideals in $\mathbb{Z}$, with bases of sizes bounded by the function values:

$$f(i+\kappa) \le f(i+1+\kappa) \le \cdots \le f(k-1+\kappa) \le f(k+\kappa) \le \cdots \le f(\ell+\kappa).$$

Then

$$\ell \le i + [f(i+\kappa)+1]$$

PROOF.
Since $\mathbb{Z}$ is a PID, each $\mathcal{M}_k$ is a principal ideal generated by a single element whose size is strictly bounded by the bound on the size of the bases of $\mathcal{M}_i$. Thus we can always find $(\ell - i)$ distinct integers whose sizes are bounded by $f(i+\kappa)$. This provides the required bound on ℓ. □

Lemma 4.11 *Assume that*

$$\mathcal{M}_i \subsetneq \mathcal{M}_{i+1} \subsetneq \cdots \subsetneq \mathcal{M}_{k-1} \subsetneq \mathcal{M}_k \subsetneq \cdots \subsetneq \mathcal{M}_\ell$$

is an ascending chain of ideals in $\mathbf{Q}[x_1]$, *with monomial bases of sizes bounded by the function values:*

$$f(i+\kappa) \leq f(i+1+\kappa) \leq \cdots \leq f(k-1+\kappa) \leq f(k+\kappa) \leq \cdots \leq f(\ell+\kappa).$$

Then

$$\ell \leq i + [f(i+\kappa)+1]$$

PROOF.
Since $\mathbf{Q}[x_1]$ is a PID, each $\mathcal{M}_k$ is a principal ideal generated by a single element whose size is strictly bounded by the bound on the size of the bases of $\mathcal{M}_i$. Thus we can always find $(\ell - i)$ distinct powers of x_1 whose sizes are bounded by $f(i+\kappa)$. This again provides the required bound on ℓ. □

In a manner first proposed by A. Seidenberg, we shall next consider a set of ascending (not necessarily strict) chains of monomial ideals, where each chain contains ideals all in $\mathbf{Z}[x_1, \ldots, x_n]$ or all in $\mathbf{Q}[x_1, \ldots, x_n, x_{n+1}]$. Furthermore, we shall assume that all the chains are of same length L, the i^{th} monomial ideal in each chain has a monomial basis whose sizes are bounded by the function value $f(i+\kappa) \leq F_K(i+\kappa)$ and that for each $i < L$, there is a chain (t^{th} chain) in the set for which $\mathcal{M}^t_i \subsetneq \mathcal{M}^t_{i+1}$. Here, the function F_K is the K^{th} function in the Wainer hierarchy and $K \geq 2$. We write such a set as follows:

$$\begin{array}{ccccccc}
\mathcal{M}^1_1 & \subseteq & \mathcal{M}^1_2 & \subseteq & \cdots & \subseteq & \mathcal{M}^1_L \\
\mathcal{M}^2_1 & \subseteq & \mathcal{M}^2_2 & \subseteq & \cdots & \subseteq & \mathcal{M}^2_L \\
 & \vdots & & & & & \\
\mathcal{M}^t_1 & \subseteq & \mathcal{M}^t_2 & \subseteq & \cdots & \subseteq & \mathcal{M}^t_L \\
 & \vdots & & & & & \\
\mathcal{M}^m_1 & \subseteq & \mathcal{M}^m_2 & \subseteq & \cdots & \subseteq & \mathcal{M}^m_L
\end{array}$$

and denote it by $\mathbf{S}(n, m, K)$, where n is its *order*, K is its *order of growth*, m is its *width* and L is its *length*. We would like to obtain a bound on the length L as a function m, n, K and κ. While each chain may not be strictly ascending, we refer to the set of chains as being strictly ascending, as we require that for each $i < L$, there is a chain (t^{th} chain) in the set for which $\mathcal{M}^t_i \subsetneq \mathcal{M}^t_{i+1}$.

It is also obvious that for each chain

$$\mathcal{M}^t_1 \subseteq \mathcal{M}^t_2 \subsetneq \cdots \mathcal{M}^t_L$$

we can construct at most $(n+1)$ chains involving *smaller order* by taking the extended ideals under the projection ring homomorphisms:

$$\begin{array}{ccccccc}
\mathcal{M}_1^{t(0)} & \subseteq & \mathcal{M}_2^{t(0)} & \subseteq & \cdots & \subseteq & \mathcal{M}_L^{t(0)} \\
\mathcal{M}_1^{t(1)} & \subseteq & \mathcal{M}_2^{t(1)} & \subseteq & \cdots & \subseteq & \mathcal{M}_L^{t(1)} \\
\vdots & & & & & & \\
\mathcal{M}_1^{t(j)} & \subseteq & \mathcal{M}_2^{t(j)} & \subseteq & \cdots & \subseteq & \mathcal{M}_L^{t(j)} \\
\vdots & & & & & & \\
\mathcal{M}_1^{t(n)} & \subseteq & \mathcal{M}_2^{t(n)} & \subseteq & \cdots & \subseteq & \mathcal{M}_L^{t(n)}
\end{array}$$

Now collecting all such ascending chains for all the t's, we obtain a new set of the same length L, same order of growth K, but of smaller order $(n-1)$ and larger width $m(n+1)$. However, such a set of ascending chains of monomial ideals is *not necessarily ascending* (as a set). Let $i_1 = 1, i_2, \ldots, i'_L \leq L$ be a set of indices such that for all t's and j's

$$\mathcal{M}_{i_\ell}^{t(j)} = \mathcal{M}_{i_\ell+1}^{t(j)} = \cdots = \mathcal{M}_{i_{\ell+1}-1}^{t(j)},$$

but for some t and j

$$\mathcal{M}_{i_{\ell+1}-1}^{t(j)} \subsetneq \mathcal{M}_{i_{\ell+1}}^{t(j)}.$$

However, one can derive a strictly ascending set of ascending chain of monomial ideals, by simply deleting the monomial ideals whose index is not among the indices $i_1, i_2, \ldots, i'_L$. However the resulting set of ascending chains has a shorter length $L' \leq L$ and growth rate given by $g(j) = f(i_j + \kappa) \leq F_{K'}(j + \kappa + n)$. The width and the order remain unchanged: $m(n+1)$ and $(n-1)$. We refer to the set of ascending chain so constructed by $\mathbf{S}'(n-1, m(n+1), K')$.

First note that:

$$i_{\ell+1} - i_\ell \leq m[f(i_\ell + \kappa) + 1]^{n+1} + 1,$$

Since otherwise, we could find an ascending chain of ideals

$$\mathcal{M}_{i'_1}^{t} \subsetneq \mathcal{M}_{i'_2}^{t} \subsetneq \cdots \subsetneq \mathcal{M}_{i'_k}^{t},$$

where $i'_1 = i_\ell$, $i'_k \leq i_{\ell+1}$ and $k > [f(i_\ell + \kappa) + 1]^{n+1} + 1$, with the property that when we consider the corresponding chains of extended ideals (under projection ring homomorphisms) they would all be equal—such as situation will directly contradict the results from the corollaries 4.8 and 4.9.

Let us now define a function $h\colon \mathbf{N} \to \mathbf{N}$ as follows:

$$\begin{array}{rcl}
h(1) & = & 1 \\
h(i) & = & i + m[f(i_\ell + \kappa) + 1]^{n+1} + 1.
\end{array}$$

It is easily seen that $i_\ell \leq h(\ell)$ and that $h(i) \leq F_{K+2}(i + \kappa + n)$. (Direct consequence of the facts 1, 2 and 3 of the section §3 and the following observation:

$$\begin{aligned}
&[f(j+\kappa)+1]^{n+1} \leq [F_K(j+\kappa+1)]^{n+1} \\
&\leq \ F_K^{(n+1)}(j+\kappa+1) \\
&\leq \ F_K^{(n+2)}(j+\kappa) \\
&\leq \ F_K^{(j+\kappa+n+1)}(j+\kappa+n) \ \leq \ F_{K+1}(j+\kappa+n) \quad).
\end{aligned}$$

Now it's easy to see that the order of growth K' of the set $\mathbf{S}'(n-1, m(n+1), K')$ is given by the function:

$$g(j) = f(h^{(j-1)}(1) + \kappa) \leq F_{K+3}(j + \kappa + n),$$

and that $K' = K + 3$. (Direct consequence of the facts 1, 2 and 3 of the section §3)

Now we claim that the following relation holds between the lengths L and L'

$$\begin{aligned} L(n,m,K) &\leq L' \cdot \left(m[f(i_{L'} + \kappa) + 1]^{n+1} + 1\right) \\ &\leq L' \cdot \left(m[g(L') + 1]^{n+1} + 1\right) \\ &\leq F_{K+4}(L' + \kappa + n) \\ &= F_{K+4}(L(n-1, m(n+1), K+3) + \kappa + n). \end{aligned}$$

Thus by repeated application of the above relation, we see that

$$L(n,m,K) \leq F^{(n)}_{K+4n+1}(L(0, m(n+1)^n, K+3n) + n \cdot F^{(n)}_{K+4n+1}(\kappa + n).$$

Now using the lemmas 4.10 and 4.11, we see that

$$L(0,m,K) \leq m[F_K(1) + 1].$$

Thus we obtain the following bound on the length of a set of ascending chain of monomial ideals, $\mathbf{S}(n, 1, K)$:

$$L(n,1,K) \leq F_{K+4n+2}(\kappa + n + 1).$$

5. Summary of Results

Now summarizing the discussions of the preceding section,

Theorem 5.12 *Let L bound the length of any ascending chain of monomial ideals of $\mathbf{Z}[x_1, \ldots, x_n]$*

$$\mathcal{M}_1 \subsetneq \mathcal{M}_2 \subsetneq \cdots \subsetneq \mathcal{M}_i \subsetneq \cdots,$$

where $\mathcal{M}_i$ has a monomial basis with coefficients and degrees bound of $F_K(i + \kappa)$. Then

$$L \leq F_{K+4n+2}(\kappa + n + 1). \quad \square$$

Now, note that the function $2 \uparrow^{(5i+\max\{c,d,n\})} \leq F_4(i + \max\{c,d,n\})$, and using this fact, we obtain the following refinement of the main theorem of section §2:

Theorem 5.13 *Let N' bound the length of any ascending chain of monomial ideals*

$$\mathcal{M}_1 \subsetneq \mathcal{M}_2 \subsetneq \cdots \subsetneq \mathcal{M}_i \subsetneq \cdots,$$

where $\mathcal{M}_i$ has a monomial basis with coefficients and degrees bound of $2 \uparrow^{(5i+\max\{c,d,n\})}$. Then

$$N' \leq F_{4n+6}(\max\{c,d,n\} + 1),$$

and our algorithm to compute an E-basis of a set of ν polynomials M $\subsetneq \mathbf{Z}[x_1, \ldots, x_n]$ *of coefficients and degrees bounds of c and d, respectively, uses no more than N arithmetic steps, where*

$$N \leq F_{4n+7}(\max\{\nu, c, d, n\} + 1).$$

Also, the resulting E-Basis has its degrees and coefficients bounded by

$$F_{4n+7}(\max\{c, d, n\} + 1). \quad \square$$

We note that while these bounds are rather crude, for a fixed n the complexity remains bounded by a function of input size whose growth rate is bounded by a primitive recursive function. However, if we consider the complexity as a function of n this bound has a growth rate similar to the Ackermann's function.

Following in a manner similar to the ones in the previous section, we obtain the following results:

Theorem 5.14 (Kronecker's Problem) *Given an ideal* $\mathcal{M} = (M_1, M_2, \ldots, M_\nu) \subset \mathbf{Z}[x_1, x_2, \ldots, x_n]$ *and a polynomial* $A \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$, *there is a decision procedure to decide the ideal membership problem (whether* $A \in \mathcal{M}$*) which requires no more than following number of steps:*

$$F_{4n+8}(\max\{\nu, n, |A|, |M_1|, \ldots, |M_\nu|\} + 1).$$

Also, given $A, A', M_1, M_2, \ldots, M_\nu \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$, *there is a decision procedure to decide whether* $A \sim A' \bmod (M_1, M_2, \ldots, M_\nu)$, *which requires no more than following number of steps:*

$$F_{4n+8}(\max\{\nu, n, |A|, |A'|, |M_1|, \ldots, |M_\nu|\} + 1).$$

Theorem 5.15 (Detachability Problem) *Given* $A, M_1, M_2, \ldots, M_\nu \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$, *let*

$$\Theta = \{\langle\theta_1, \ldots, \theta_\nu\rangle : A = \theta_1 M_1 + \cdots \theta_\nu M_\nu\}.$$

If $\Theta \neq \emptyset$ *then*

$$\min\{\max\{|\theta_1|, \ldots, |\theta_\nu| : \langle\theta_1, \ldots, \theta_\nu\rangle \in \Theta\}\} \leq F_{4n+8}(\max\{\nu, n, |A|, |M_1|, \ldots, |M_\nu|\} + 1). \quad \square$$

Theorem 5.16 (An Effective Hilbert's Basis Theorem) *Let L bound the length of any ascending chain of ideals of* $\mathbf{Z}[x_1, \ldots, x_n]$

$$\mathcal{M}_1 \subsetneq \mathcal{M}_2 \subsetneq \cdots \subsetneq \mathcal{M}_i \subsetneq \cdots,$$

where $\mathcal{M}_i$ *has a basis with coefficients and degrees bound of* $F_K(i)$. *Then*

$$L \leq F_{K+8n+10}(n + 1).$$

PROOF.

Consider the following ascending chain of monomial ideals of $\mathbf{Z}[x_1, \ldots, x_n]$

$$\text{Head}(\mathcal{M}_1) \subsetneq \text{Head}(\mathcal{M}_2) \subsetneq \cdots \subsetneq \text{Head}(\mathcal{M}_i) \subsetneq \cdots$$

By the preceding arguments, we know that the

$$\{\text{Hmono}(M) : M \in E\text{-basis}(\mathcal{M}_i)\}$$

is a basis for the head monomial ideal Head($\mathcal{M}_i$) with degrees and coefficients bounded by $F_{4n+7}(F_K(i) + 1) \leq F_{K+4n+8}(i)$. Thus the length of the ascending chain of head monomial ideals is bounded by

$$F_{K+4n+8+4n+2}(n+1).$$

But since $\mathcal{M}_i \subsetneq \mathcal{M}_{i+1}$ implies that Head($\mathcal{M}_i$) $\subsetneq$ Head($\mathcal{M}_{i+1}$), we see that

$$L \leq F_{K+8n+10}(n+1). \quad \square$$

Acknowledgement

We wish to acknowledge with gratitude the many rewarding conversations with Professors H.M. Edwards and R. Pollack both of Courant Institute. In particular, Professor Edwards had posed the problem to us and helped us considerably in formulating the problem and the solution reported here.

Appendix 1. Expansion Algorithm and the Bounds

In this appendix, we describe a simple algorithm to compute $\psi(\mathrm{M}')$ of a non-empty subset $\mathrm{M}' = \{M_1', \ldots, M_\mu'\} \subset \mathbf{Z}[x_1, x_2, \ldots, x_n]$. The algorithm is based on a simple generalization of the classical Euclid's algorithm. Later on, in the appendix, we shall provide somewhat crude but simple complexity bounds on the number of steps the algorithm takes as well as the coefficient and degree bounds for the resulting polynomials.
We recall that since $\mathbf{Z}$ is an Euclidean Domain, it supports the following
Division Algorithm:

$$(\forall s, t \in \mathbf{Z}, s \neq 0)\,(\exists q, r \in \mathbf{Z}) \qquad t = q \cdot s + r, \qquad (q = \text{quotient},\ r = \text{remainder}),$$

in which either $r = 0$ or $|r| < |s|$. Additionally, if we assume that $|q|$ takes the smallest possible value, then the quotient and the remainder are uniquely determined, and $|q| < |t|$.
The algorithm is now as follows:

```
Expansion:

Input:    $\mathrm{M}' = \{M_1', M_2', \ldots, M_\mu'\}$.
Output:   $\psi(\mathrm{M}')$.
          Assume that $|\mathrm{Hcoef}(M_1')| \le |\mathrm{Hcoef}(M_2')| \le \cdots \le |\mathrm{Hcoef}(M_\mu')|$;
          Insert the following elements into a queue $Q$;
          $(w_{1,1}, \ldots, w_{1,\mu}; w_1) := (1, 0, \ldots, 0; \mathrm{Hcoef}(M_1'))$;
          $(w_{2,1}, \ldots, w_{2,\mu}; w_2) := (0, 1, \ldots, 0; \mathrm{Hcoef}(M_2'))$;
                    ⋮
          $(w_{\mu,1}, \ldots, w_{\mu,\mu}; w_\mu) := (0, 0, \ldots, 1; \mathrm{Hcoef}(M_\mu'))$;

          while $|Q| > 1$ loop
              Dequeue the following first two elements of the queue $Q$:
                  $(w_{1,1}, \ldots, w_{1,\mu}; w_1)$ and $(w_{2,1}, \ldots, w_{2,\mu}; w_2)$;
              Let $w_2 = q \cdot w_1 + r$;

              Enqueue $(w_{1,1}, \ldots, w_{1,\mu}; w_1)$ in the queue $Q$;
              if $r \neq 0$ then
                  Enqueue $(w_{2,1}, \ldots, w_{2,\mu}; w_2) - q \cdot (w_{2,1}, \ldots, w_{2,\mu}; w_2)$;
              end if ;
          end loop ;
          Let $\pi = \mathrm{LCM}\left\{\mathrm{Hterm}(M_1'), \ldots, \mathrm{Hterm}(M_\mu')\right\}$;
          return $w_{1,1} \frac{\pi}{\mathrm{Hterm}(M_1')} M_1' + \cdots + w_{1,\mu} \frac{\pi}{\mathrm{Hterm}(M_\mu')} M_\mu'$;
end Expansion.  □
```

The correctness and termination of the algorithm follows from the following easily verifiable facts. Assume that at the beginning of each iteration the queue Q contains the following t $(2 \leq t \leq \mu)$ elements

$$\begin{aligned}\bar{w}_1 &= (w_{1,1}, \ldots, w_{1,\mu}; w_1),\\ \bar{w}_2 &= (w_{2,1}, \ldots, w_{2,\mu}; w_2),\\ &\vdots\\ \bar{w}_t &= (w_{t,1}, \ldots, w_{t,\mu}; w_t).\end{aligned}$$

Then

1. $|w_1| \leq |w_2| \leq \cdots \leq |w_t| \leq |\text{Hcoef}(M'_\mu)|$.
2. $\gcd\Big\{w_1, \ldots, w_t\Big\} = \gcd\Big\{\text{Hcoef}(M'_1), \ldots, \text{Hcoef}(M'_\mu)\Big\}$.
3. For all j $(0 \leq j \leq t)$

$$w_j = w_{j,1} \cdot \text{Hcoef}(M'_1) + \cdots + w_{j,\mu} \cdot \text{Hcoef}(M'_\mu).$$

Furthermore, if the queue $Q = [\bar{w}_1, \ldots, \bar{w}_t]$ before the main loop and $Q' = [\bar{w'}_1, \ldots, \bar{w'}_{t'}]$ at the end of the main loop, then

1. $|w_1| \geq |w'_1|$ or $t \geq t'$ and at least one of the inequalities is strict;
2. Since $|q| < |w_2| \leq |\text{Hcoef}(M'_\mu)|$,

$$|w'_{i,j}| \leq \max_{k,l}\{|w_{k,l}|\} \cdot |\text{Hcoef}(M'_\mu)|.$$

Thus the algorithm uses at most $\mu + |\text{Hcoef}(M'_1)|$ iterations of the loop, and the the multipliers, $w_{i,j}$'s are bounded by

$$(|\text{Hcoef}(M'_\mu)|)^{|\text{Hcoef}(M'_1)|-1}.$$

Thus, if we assume that c and d, respectively, bound the coefficients and degrees (in each variable) of the polynomials in M' then c^c and $2d$ bound the coefficients and degrees of the polynomials in $\psi(\mathrm{M}')$. The algorithm uses at most $\mu^2 + 4\mu c + \mu(d+1)^n$ arithmetic steps. In summary,

Theorem 0.17 *Let* $\mathrm{M} = \{M_1, M_2, \ldots, M_\nu\}$ *be a subset of polynomials in* $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ *such that their coefficients and degrees are bounded respectively by* c *and* d*. Then the* Ψ *expansion of* M, $\Psi(\mathrm{M})$, *consisting of at most* $2^\nu - 1$ *polynomials, can be computed with* $2^\nu(\nu^2 + 4\nu c + \nu(d+1)^n)$ *arithmetic steps, and their coefficients and degrees are bounded respectively by* c^c *and* $2d$. □

Appendix 2. Reduction Algorithm and the Bounds

In this appendix, we shall provide simple complexity bounds on the number of steps required by the reduction algorithm as well as the coefficient and degree bounds for the normal form of the polynomial undergoing the reduction sequence. The techniques employed here were first used by Mishra and Yap[39], and later extended by Dubé, Mishra and Yap[40].

Consider a subset $\mathrm{M} = \{M_1, \ldots, M_\nu\} \subset \mathbf{Z}[x_1, x_2, \ldots, x_n]$, with respect to which the reduction is assumed to be carried out. Further, assume that c and d, respectively, bound the coefficients and degrees (in each variable) of the polynomials in M.

If $\pi = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ is an arbitrary power product then we assign it a weight as follows:

$$\mathcal{W}_{\mathrm{M}}(\pi) = \alpha_1(d+1)^{n-1} + \alpha_2(d+1)^{n-1} + \cdots + \alpha_n(d+1)^0.$$

Note that

1. If the degrees of a power product π are bounded by D then its weight $\mathcal{W}_{\mathrm{M}}(\pi)$ is bounded by
$$\frac{D}{d}\Big((d+1)^n - 1\Big).$$

2. Conversely, if the weight a power product π is bounded by W then
$$\begin{aligned} \deg_{x_1}(\pi) &\leq \frac{W}{(d+1)^{n-1}}, \\ \deg_{x_2}(\pi) &\leq \frac{W}{(d+1)^{n-2}}, \\ &\vdots \\ \deg_{x_n}(\pi) &\leq W. \end{aligned}$$
Thus, the number of distinct power products of weights bounded by W is never bigger than
$$\frac{\Big(W + (d+1)^{n-1}\Big)^n}{(d+1)^{n(n-1)/2}}.$$

Consider a polynomial $A \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$ coefficient and degree bounds of C and D respectively. Let the weight of a multivariate polynomial be defined to be the biggest of the weights of its power products; that is,

$$\text{if } A = a_1\pi_1 + a_2\pi_2 + \cdots + a_\ell\pi_\ell \quad \text{then } \mathcal{W}_{\mathrm{M}}(A) = \max_i \mathcal{W}_{\mathrm{M}}(\pi_i).$$

[39] Bud Mishra and Chee Yap. *Notes on Gröbner Bases*, *Information Sciences*, 48, (1989), pp. 219-252

[40] Thomas Dubé, Bud Mishra and Chee Yap. *Admissible Orderings and Bounds for Gröbner Basis Normal Form Algorithms*, Courant Technical Report 258, (1986), 29pp.

Note that for every power product π and $M_i \in \mathrm{M}$,

$$\mathcal{W}_{\mathrm{M}}(\pi M_i) = \mathcal{W}_{\mathrm{M}}(\pi \mathrm{Hterm}(M_i)).$$

Using the above observations, we see that if $A \xrightarrow{M_i} A'$ then

$$A' = A - \frac{\mathrm{Hmono}(A)}{\mathrm{Hmono}(M_i)} M_i, \quad \mathrm{Hterm}(A) \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A'),$$

and

$$\begin{aligned} \mathcal{W}_{\mathrm{M}}(A') &\leq \max\left\{\mathcal{W}_{\mathrm{M}}(A), \mathcal{W}_{\mathrm{M}}\left(\frac{\mathrm{Hmono}(A)}{\mathrm{Hmono}(M_i)} M_i\right)\right\} \\ &= \max\{\mathcal{W}_{\mathrm{M}}(A), \mathcal{W}_{\mathrm{M}}(\mathrm{Hmono}(A))\} = \mathcal{W}_{\mathrm{M}}(A). \end{aligned}$$

Additionally, the coefficients and degrees of A' are bounded respectively by Cc and $D + d$. But just from the considerations of weights, we also observe that the degrees of A' are bounded by $\mathcal{W}_{\mathrm{M}}(A) = \frac{D}{d}((d+1)^n - 1)$.

Now, extending the above arguments to a reduction sequence, we see that if

$$A \xrightarrow{\mathrm{M}} A_1 \xrightarrow{\mathrm{M}} \cdots \xrightarrow{\mathrm{M}} A_j \xrightarrow{\mathrm{M}} A',$$

then

$$\mathrm{Hterm}(A) \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A_1) \underset{\mathrm{lex}}{>} \cdots \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A_j) \underset{\mathrm{lex}}{>} \mathrm{Hterm}(A'),$$

and each of them has a weight bounded by $\mathcal{W}_{\mathrm{M}}(A) \leq \frac{D}{d}((d+1)^n - 1)$.

Thus the length of the reduction, $j + 1$ is bounded by the number of distinct power products of weight no larger than $\mathcal{W}_{\mathrm{M}}(A)$, i.e.,

$$j + 1 \leq \left(\frac{D}{d} + 1\right)^n (d+1)^{n(n+1)/2}.$$

Furthermore, the coefficients and degrees of A' are bounded, respectively, by

$$Cc^{(D/d+1)^n (d+1)^{n(n+1)/2}} \quad \text{and} \quad \left(\frac{D}{d}\right)\left((d+1)^n - 1\right).$$

Theorem 0.18 *Let* $\mathrm{M} = \{M_1, M_2, \ldots, M_\nu\}$ *be a subset of polynomials in* $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ *such that their coefficients and degrees are bounded respectively by c and d. Then, for any two distinct polynomials* M_i *and* M_j,

1. *The coefficients and degrees of* $S(M_i, M_j)$ *are bounded by* c^2 *and* $2d$.
2. $\mathrm{NF}_{\mathrm{M}}(M_i, M_j)$ *can be computed with at most* $3^{2n}(d+1)^{n(n+1)}$ *arithmetic steps, and its coefficients and degrees are bounded respectively by*

$$c^{2+3^n (d+1)^{n(n+1)/2}} \quad \textit{and} \quad 2(d+1)^n. \quad \square$$

NYU COMPSCI TR-600 c.1
Gallo, Giovanni
A solution to Kronecker's
problem.

NYU COMPSCI TR-600 c.1
Gallo, Giovanni
A solution to Kronecker's
problem.

DATE DUE	BORROWER'S NAME

LIBRARY
N.Y.U. Courant Institute of
Mathematical Sciences
251 Mercer St.
New York, N. Y. 10012

This book may be kept

FOURTEEN DAYS

A fine will be charged for each day the book is kept overtime.
